

UNCLASSIFIED

RECON Guard Phased Delivery
(13 March 1984)

ATTACHMENT A

UNCLASSIFIED

RECON GUARD Phased Delivery Configurations and Schedule

This document serves to describe phases in the delivery of the RECON GUARD system.

Listed below are the phases and a short description of each. Phases 1 through 7 have been completed.

- Phase 1: COMTEN Electrical Characteristics Verification.
To determine exact electrical characteristics.
- Phase 2: Mountain View Acceptance Tests.
To conduct acceptance tests prior to shipment.
- Phase 3: Completion of Online Guard ICD.
To determine and specify the Guard/RECON interface by actual measurements of RECON.
- Phase 4: Guard System Installation and On-Site Acceptance Testing.
To install equipment in the RCC and assure correct operation following delivery.
- Phase 5: New Data Side / GTS development.
Alteration of the OLG Data Side sbc to perform according to the October 14 ICD.
- Phase 6: Conformation of Protocol Converter.
To assure correct operation of selected protocol converter as installed in the RCC.
- Phase 7: Initial RECON Connection.
To connect the Online Guard to RECON and observe the results.

Phase 8 is underway.

- Phase 8: Interface to RECON.
To provide operational interconnection of the Online Guard to RECON for use in Customer confidence testing.

Guard Phased Delivery

Phases 9 and 10 are not completed, largely sequential, and do not depend on previous phases (except for system installation, Phase 4).

Phase 9: Initial HAS Connection.
To connect the Online Guard to HAS and observe the results.

Phase 10: Interface to HAS.
To provide operational interconnection of the Online Guard to HAS.

Phase 11 has been completed.

Phase 11: Delivery of Online Guard Variants.
To connect and test the operation of response counting and multiple low side Guard variants.

Other interesting events and dates are as follows:

♦ Delivery of user documentation	- January 20, 1984
♦ Delivery of source code listings	- January 20, 1984
	April 20, 1984
♦ Delivery of verification document	- April 27, 1984
♦ Delivery of revised specifications	- May 28, 1984

Guard Phased Delivery

The following schedule indicates the time frame for each phase:

PHASE	DESCRIPTION	Jan	Feb	Mar	Apr	May	Jun
		1234	1234	12345	1234	1234	1
4	Guard Installation and Acceptance Test	**					
5	New Data Side/GTS development	***					
6	Conformation of protocol converter	****					
7	Initial RECON Connection	****					
8	Interface to RECON			*****			
* 9	Initial HAS Connection	---					
* 10	Interface to HAS		----				
11	Delivery of Online Guard Variants			*			
	Delivery of user documentation		*				
	Delivery of source code listings		* (prelim)			* (final)	
	Delivery of verification document					*	
	Delivery of revised specifications					*	
		1234	1234	12345	1234	1234	1
			1234		1234		
		Jan	Feb	Mar	Apr	May	Jun

(*) These phases are HAS dependent and are not required to fulfill Guard Program technical and security objectives.

Guard Phased Delivery

The following mnemonics are used throughout:

SOID	-----	Security Officer Interface Device.
UDG	-----	Update GUARD.
OLG	-----	Online GUARD.
PC	-----	Async to bisync protocol converter.
GTS	-----	GUARD Test System.
LANRS	-----	Local Area Network Research System.
JES/MVS	-----	IBM operating system.
ICD	-----	Interface Control Document.
INTERVIEW 4500	-	Diagnostic test equipment.
BREAKOUT BOX	-	Diagnostic test equipment.

Guard Phased Delivery

PHASE 1 -- COMTEN Electrical Characteristics Verification

Objective:

To determine exact electrical characteristics of the
COMTEN/RECON connection by Sytek personnel.

Completion date:

September 1, 1983

Results:

Electrical characteristics were satisfactorily determined which
enabled proceeding with Phase 3.

```
-----  
| Interview 4500 |---| COMTEN |---| JES |---| RECON |  
-----
```

Guard Phased Delivery

PHASE 2 -- Mt. View Acceptance Tests

Objective:

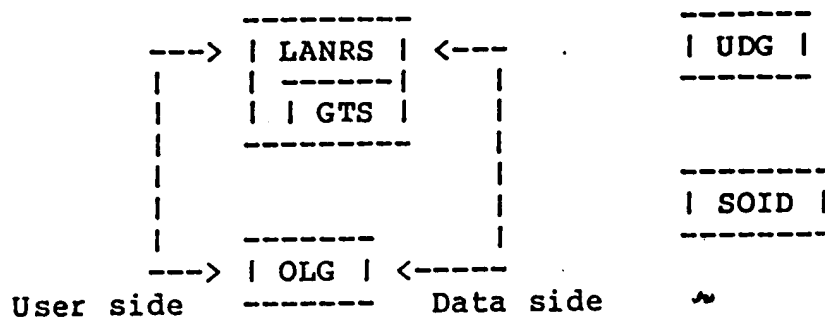
To conduct acceptance testing of the Guard System and GTS prior to shipment. Successful completion of this phase indicates the Guard System and GTS have properly implemented the design objectives as contained in the Sytek produced specifications documents approved by the Customer.

Completion date:

October 19, 1983.

Procedures:

The following equipment configuration was used for acceptance testing:



Results: Acceptance tests were conducted by customer designated personnel using customer data provided for that purpose. Acceptance testing of the Guard System include all items of the SYTEK TR-82016 "Test/Evaluation Plan and Procedures" dated 30 April 1982, Sections 3 and 4, plus items specified by the J.P. Anderson "Proposed Acceptance Tests for RECON Guard" dated 20 February 1983.

Following satisfactory completion of acceptance tests, the SOID, UDG, OLG, and GTS were prepared for shipment to the customer's site.

Guard Phased Delivery

PHASE 3 --- Completion of OLG ICD

Objective:

To derive and document a complete and correct Interface Control Document utilizing results and information gained from analysis and testing of the original ICD and actual COMTEN/RECON connections.

Completion date:

October 14, 1983.

Results:

By actual low level monitoring and modulation of the COMTEN cable connection, Sytek personnel have determined the correct characteristics of the following items:

- ♣ The format of batch requests made by OLG to RECON.
- ♣ A wide variety of responses from COMTEN/RECON other than RECON linear records (IAT messages and other special responses).
- ♣ JES definition of OLG as RM100, RM101, and RM102 was verified.
- ♣ The relationship of COMTEN/RECON responses to transparent and non-transparent bisync protocols were investigated.

Guard Phased Delivery**PHASE 4 -- Guard System Installation and On-Site Acceptance Testing****Objective:**

Installation of the SOID, UDG, OLG and GTS in the RCC. Repetition of Acceptance tests to ensure safe transit and delivery of proper equipment and software.

Performance Period:

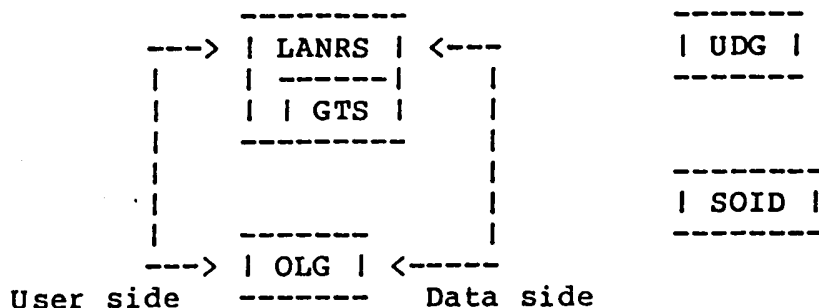
December 12, 1982 through January 13, 1983

Requirements:

- ◆ Site properly prepared to accommodate GUARD hardware configuration. Government furnished equipment in place.
- ◆ Arrival of all shipped equipment in satisfactory condition.
- ◆ Customer provided escort of Sytek personnel.

Procedures:

The following initial equipment configuration will be used for on-site acceptance tests:



Acceptance tests conducted will be the same as those used in Phase 2.

Guard Phased Delivery

PHASE 5 --- New Data Side / GTS Development

Objective:

To design, build and test a data side OLG slave which meets the ICD completed in Phase 3.

Start date:

December 5, 1983

Estimated completion date:

January 20, 1984.

Requirements:

- ◆ Access to operational COMTEN/RECON connections.
- ◆ Access to customer personnel knowledgeable in COMTEN/JES/RECON system level problem solving.
- ◆ Substantial progress on phase 6 (Conformation of protocol converter).
- ◆ Customer provided escort of Sytek personnel (if access is necessary).

Procedures:

New data side code will be developed in Mountain View to the October 14, 1983 ICD. Upon satisfactory performance of the acceptance tests with the GTS simulating both HAS and RECON, the new data side and GTS code will be sent to the customer's location where testing may begin using the actual HAS and COMTEN/RECON connections and selected protocol converter.

Guard Phased Delivery

PHASE 6 --- Conformation of Protocol Converter

Objective:

To select and test a protocol converter that will properly connect the OLG asynchronous Data Side to the bisynchronous transparent/non-transparent COMTEN/RECON connection.

Performance Period:

January 3, through January 27, 1984

Requirements:

- ◆ Access to operational COMTEN/RECON connections.
- ◆ Access to customer personnel knowledgeable in COMTEN/JES/RECON system level problem solving.
- ◆ Customer provided escort of Sytek personnel.

Procedures:

Sytek personnel will use diagnostic equipment connected to the protocol converter and COMTEN/RECON as indicated below. Tests will be performed to determine correct operation of the following:

- ◆ Support of both transparent and non-transparent protocols.
- ◆ Bidirectional data transmissions.
- ◆ Bidirectional flow control function from both bisync and async ports.

Test Configuration 1:

```
-----  
| ASCII TERM |--| BREAKOUT BOX |--| PC |--| INTERVIEW 4500 |  
-----
```

Test Configuration 2:

```
-----  
| INTERVIEW 4500 |--| PC |--| COMTEN |--| JES |--| RECON |  
-----
```

Guard Phased Delivery

PHASE 7 -- Initial RECON Connection

Objective:

To examine the results of first connecting test equipment, and then the the OLG Data Side code to RECON through the protocol converter and observing results with emphasis on developing the correct interface at both application and lower protocol levels.

Data obtained in this phase may necessitate changes in the OLG Data Side code and spawn further iterations. No substantial changes are anticipated.

Start date:

January 23, 1984

Estimated completion date:

February 17, 1984.

Requirements:

- ◆ COMTEN/RECON connections present.
- ◆ COMTEN/RECON ports correctly configured by the customer
- ◆ Completion of Phase 4 installation and acceptance tests.
- ◆ Access to customer personnel knowledgeable in COMTEN/JES/RECON system level problem solving.
- ◆ Customer provided escort of Sytek personnel.

Procedures:

The following hardware configurations will be used:

Guard Phased Delivery**PHASE 7 hardware configurations:****Test Configuration 1:**

```

-----
| HAS | (No connection made)
-----

```

```

-----
| INTERVIEW 4500 |--| PC |--| COMTEN |--| JES |--| RECON |
-----

```

Test Configuration 2:

```

-----
| HAS | (No connection made)
-----

```

	User Side	Data Side						
	LANRS		OLG		PC		COMTEN	
	-----		-----		-----		-----	
	GTS							

Guard Phased Delivery**PHASE 8 -- Interface to RECON****Objective:**

To provide operational interconnection of the OLG with RECON for use in customer confidence testing.

Start date:

March 19, 1984

Estimated completion date:

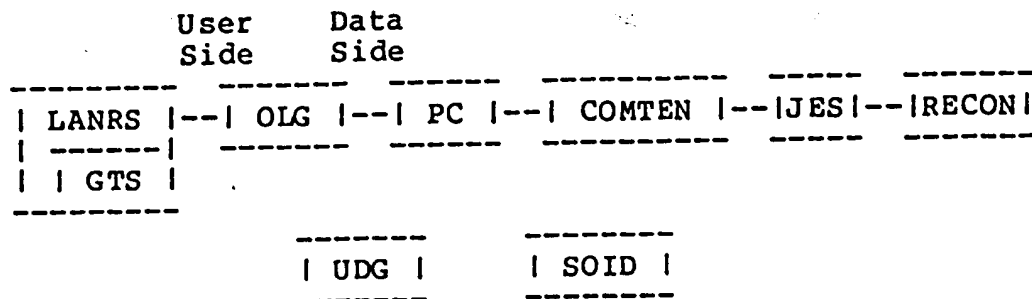
April 13, 1984

Requirements:

- ◆ Successful completion of prior phases.
- ◆ Identification of appropriate request records to test all aspects of the Guard/COMTEN interface. (This will require Sytek and Customer participation.)
- ◆ Access to customer personnel knowledgeable in COMTEN/JES/RECON system level problem solving.
- ◆ Customer provided escort of Sytek personnel.

Procedures:

The following hardware configuration will be used:



Note: An unclassified subset of the RECON Data Base will be used for this and all subsequent tests.

Note that the GTS is used in the HAS simulation mode. Sufficient request records are created on the GTS system during this period and submitted to RECON via the Guard to allow customer testing.

Guard Phased Delivery**PHASE 9---Initial HAS Connection****Objective:**

To examine the results of first connecting test equipment, and then the OLG to the HAS connection and observing the results. Data obtained in this phase may necessitate changes in the OLG User Side and spawn further iterations.

Start date:

Immediately following HAS installation.

Estimated completion date:

Three weeks from start date.

Requirements:

- ◆ HAS and HAS connections present.
- ◆ HAS interface software conforming to Sytek specifications provided with HAS.
- ◆ Completion of Phase 4 installation and acceptance tests.
- ◆ Access to contractor knowledgeable in HAS system level problem solving.
- ◆ Customer provided escort of Sytek personnel.

Procedures:

The following hardware configurations will be used:

Test Configuration 1:

```

-----
| HAS |---| INTERVIEW 4500 |
-----

```

(No connection made)

```

-----
| COMTEN |--|JES|--|RECON|
-----

```

Test Configuration 2:

```

               User   Data
               Side   Side
-----
| HAS |---| LANRS |--| OLG |---
-----
| | GTS |
-----
|
-----

```

(No connection made)

```

-----
| COMTEN |--|JES|--|RECON|
-----

```

Guard Phased Delivery

PHASE 10 --- Interface to HAS

Objective:

To provide an operational interface between the HAS and the Guard for confidence testing.

Start date:

Upon completion of Phase 9, Initial HAS Connection:

Estimated completion date:

Dependent on HAS availability (approximately 4 weeks).

Requirements:

- ◆ HAS connections present.
- ◆ HAS interface software conforming to Sytek specifications provided with HAS.
- ◆ Successful completion of prior phases.
- ◆ Access to contractor and or customer personnel knowledgeable in HAS system level problem solving.
- ◆ Customer provided escort of Sytek personnel.

Procedures:

The following hardware configurations will be used:

Guard Phased Delivery**PHASE 10 hardware configurations:****Test Configuration 1:**

(No connection made)

```

-----
| COMTEN |--|JES|--|RECON|
-----

```

		User Side	Data Side
TERM --	HAS ---	LANRS --	OLG ---
		GTS	

Test Configuration 2:

(No connection made)

```

-----
| COMTEN |--|JES|--|RECON|
-----

```

		User Side	Data Side
COINS --	HAS ---	LANRS --	OLG ---
		GTS	

Note: This testing will be conducted in two parts. In the first part queries will be submitted from a terminal directly connected to the HAS. In the second part queries will be submitted across the COINS Test Subnet. AT NO TIME WILL CLASSIFIED RECON RECORDS BE EXPOSED TO THE OPERATIONAL COINS NETWORK (Unless specifically approved by the participating Office Directors through the DCI).

Guard Phased Delivery

PHASE 11 -- Delivery of Online Guard Variants

Objective:

Following correct operation of the basic OLG, the response counting and multiple low side OLG variants will be integrated and tested at the customer's site.

Start date:

Upon completion of Phase 7 (Initial RECON Connection).
March 12, 1984.

Estimated completion date:

March 19, 1984.

Requirements:

- ◆ HAS connections present, or GTS in HAS simulation mode.
- ◆ RECON connections present.
- ◆ Access to contractor and or customer personnel knowledgeable in HAS system level problem solving (if HAS is to be used).
- ◆ Customer provided escort of Sytek personnel.

Procedures:

The following hardware configurations will be used:

Guard Phased Delivery**PHASE 11 hardware configurations:****Test Configuration 1: Response Counting Mode.**

(No connection made)

```

-----
| COMTEN |--|JES|--|RECON|
-----

```

```

                                     User   Data
                                     Side   Side
-----
| COINS |--| HAS |---| LANRS |--| OLG |---|
-----
| | GTS |
-----
|
-----

```

Test Configuration 2: Multiple Low Side Mode.

(No connection made.)

```

-----
| COMTEN |--|JES|--|RECON|
-----

```

```

                                     User
                                     Side
-----
| HAS |-----|
-----
| LANRS |---| OLG |---|
| -----|
| | GTS | User
|-----| Side
|
-----

```

UNCLASSIFIED

RECON/Guard Confidence Tests
(3 January 1983)

ATTACHMENT B

UNCLASSIFIED

Introduction

The purpose of this document is to identify the objectives, methods, and acceptable results of the RECON Guard program acceptance test phase.

The tests outlined here will be conducted by government personnel. Many of the tests will utilize a test Trap-Door program. This Trap-Door program will be generated by OCR/IAB and is specified in this document.

RECON Guard System Acceptance Tests

(Overview)

Objective:

The objective of the Government acceptance tests is the determination of the Guard System's ability to perform its security functions in the presence of normal and abnormal perturbation of the expected/standard operating environment.

Security Vulnerability Determination:

- . Operational tests
 - incorrect key insertion/removal
 - induced errors on on-line and update Guard I/O modules (i.e., can record incorrectly written on output tape of update Guard be inadvertently released?)
 - establish ideal setting for variable Guard System parameter
- . Guard System outage tests
 - random stop/start during record transmission
 - other induced Guard System errors
- . Covert signalling channel tests attempt to transmit data by:
 - modulation of handshake sequence
 - modulation of error messages
 - modulation of legitimate traffic (intact RECON records)
 - alteration of record content
- . Composite tests

All tests will be conducted by or in the presence of designated Government personnel.

Each test or set of tests will be documented prior to the Guard System test subphase. This documentation will include the following:

- . objective
- . method
- . acceptable results

System Outage Testing/Operational Testing

Objective:

The objective of these tests will be to determine the reliability and stability of the Guard System under normal and abnormal/hostile conditions.

Method:

The operational tests will be ongoing during the entire acceptance testing phase. These operational tests will include such actions as would be encountered during operation of the Guard System. These actions will include the following:

1. Random unplugging of On-Line and Up-Date Guard.
2. Random switching/removal of AGB's
 - a. during operation periods
 - b. between operation periods
3. Disruption of Security Officer Interface system
 - a. by random/intermittent power-down
 - b. incorrect keyboard entries
 - c. etc.
4. Inducement of tape errors for Up-Date Guard.
5. Other disruptive events.

Successful Results:

The Guard System should continue its security function under all circumstances. Regardless of the disruptive tests applied, the Guard System should not permit any unauthorized release of information.

Hardware Component Verification Test

Objective:

The objective of this test is to ensure, as thoroughly as possible, that no clandestine hardware (i.e., tap devices) is included in the Guard System hardware set. This hardware set includes the On-Line Guard SBC's, the Up-Date Guard SBC's, all AGB's, and Security Officer Interface hardware.

Method:

The method applied for this test will be visual inspection. More elaborate methods (i.e., IR) will be possible only if an appropriate system is available. Inspection of microprocessor chips will entail magnification and comparison (visually) with proper chip layout description.

Successful Result:

A one-to-one comparison of SBC components and, where possible, chip layout inspection for computer-on-chip components will be deemed acceptable.

Handshake Sequence Modulation

Objective:

The objective of this test will be the transmission of clandestine information by selective interrupt of HAS-Guard and RECON-Guard software communications sequence in a codable repetitive manner. The communication sequence will be interrupted (error condition) in such a way as to encode the test character string.

Method:

The handshake interrupt will be attempted both from the 370 (RECON System) operator console and (if practical) from small embedded in RECON trap door software routines. Modulation of error interrupts will use the following techniques:

1. time lapse between error interrupts
2. device interrupt error type
3. # interrupts/time period
4. use of CANCEL and STATUS acknowledge

The receiving station for this test will be on the outbound (HAS) side of the On-Line Guard device.

Acceptable Results:

The On-Line Guard device should abort all transmission (execute a channel shutdown), prior to the receipt of the full test sequence at the outbound receiving station.

Error Message Modulation

Objective:

The objective of this test is to use error messages to transmit clandestine information through the On-Line Guard device to the COINS network.

Method:

The Trap-Door program will be used to generate and transmit error messages to the COINS network. These error messages will be transmitted via the operator control mode of the Trap-Door program. A predetermined test character sequence will be the object of this method.

Acceptable Results:

The On-Line Guard device should terminate channel activity prior to output of the full test character sequence.

Alteration of Records

Objective:

The objective of this test will be the transmission of clandestine information through the On-Line Guard device by overlaying such information on legitimate outbound RECON records.

Method:

The Trap-Door program will insert predetermined character strings into authenticated RECON records. These records will then be transmitted to the On-Line Guard device for output to the COINS network.

Acceptable Results:

The On-Line Guard device should detect all such unauthorized alterations of the legitimate RECON records. The On-Line Guard should then block transmission of the altered records and inform the audit and alarm devices.

Legitimate Traffic Modulation

Objective:

The objective of this test will be the transmission of a designated character string by the use of properly authenticated records. This test will attempt to open a covert signaling channel with legitimate message traffic.

Method:

Transmit 26 properly authenticated, "correct" records to HAS. Then, as part of the same response retransmit the 25th, 15th, 21st, 8th, 1st, 22nd, 5th, 2nd, 5th, 5th, 14th, 8th, 1st, 4th, then end of response. If possible, the first 26 records should be the shortest available.

Successful Result:

The Guard will immediately recognize a direct channel attack and shut down on the receipt of the 27th record. (Actually, if it did, it would be in error of some kind.)

Also, allowable response set limit, or retransmission limit should be exceeded and cause Guard cutoff.

RECON Test (Trap-Door) Program

Objective:

The objective of the RECON acceptance test Trap-Door program will be the introduction of security relevant errors and perturbation into the Guard-RECON-HAS function. The Trap-Door program should allow the 370 system (RECON host) operator to control error condition generation from the control console. Also, the Trap-Door program should have the capability to automatically generate RECON system errors.

Function:

1. Change contents of RECON record by the following methods:
 - a. single bit change in RECON record
 - b. overlay of character string in RECON record text
2. Transmit selected error messages by:
 - a. insertion in response record set
 - b. direction from operator console
3. Transmit response record set
 - a. response record set should include altered records
 - b. response record set transmission should be under console operator control
4. Automatic execution mode
 - a. program should automatically loop through any combination of above functions
 - b. selected functions will be determined by operator at initiation of automatic execution mode
5. Simulate RECON system outages
 - a. transmit CANCEL messages under operator control
 - b. transmit CANCEL messages via automatic loop

- c. transmit status acknowledgement messages under operator control
- d. transmit status acknowledgement via automatic loop

The RECON test program should have a control structure which permits execution of all five of the above functions by two separate modes. These control modes are:

1. Automatic function execution mode
2. Operator-controlled function execution mode

Automatic Function execution mode will be RECON test program initiation of operator-selected functions in a loop method. Execution will be stopped by a preset timer, loop parameter, or operator intervention. The operational scenario will be as follows:

- a. operator parameter entries
 - (1) functions to be executed
 - (a) order of execution
 - (b) random order of execution
 - (2) stop parameters
 - (a) time
 - (b) # of execution loops
 - (c) infinite loop (stopped by operator intervention)

Operator-controlled function execution mode will be RECON test program execution of specific operator-selected functions. The operational scenario will be as follows:

- a. operator parameter entries
 - (1) functions to be executed
 - (2) # of executions

UNCLASSIFIED

Community RECON ERROR Generator
(Program Specifications)

ATTACHMENT C

UNCLASSIFIED

COMMUNITY RECON ERROR GENERATOR

This paper outlines the specifications of an error generating program developed as part of an effort to test the ability of the RECON GUARD device to detect and flag RECON records which have been altered since the assignment of a 'CHECKSUM' (by the UPDATE GUARD device). The program operates in an IBM batch environment and is written in the IBM ASSEMBLER language. The purpose of the program is to intercept and alter a COMMUNITY RECON output file prior to being received by an ONLINE GUARD device for channeling back to the COMMUNITY RECON user.

The program has been designed to be inserted into the COMMUNITY RECON job stream after the final output data set has been created but before sending the output to the ONLINE GUARD device. Through the use of Control card input the program can alter any or all of five (5) output records. The records that can be affected are:

- 1) the FIRST-CARD
- 2) the 1st RECON record
- 3) the MIDDLE RECON record
- 4) the LAST RECON record
- 5) the LAST-CARD

The program accepts any of 7 Control card formats in any order. The number of Control cards has been limited (arbitrarily) to 20. Each type of format can be used any number of times (limited to a total of 20 Control cards) and the same record can be altered with several different Control cards. The 7 general 'commands' are:

- 1) USERID -- change the userid on the FIRST-CARD
- 2) AGENCY -- change the originating agency on the FIRST-CARD
- 3) REQNUM -- change the 4 digit request number on the FIRST-CARD and LAST-CARD
- 4) BIT -- flip a single bit in the RECON record
- 5) BYTE -- alter a character in RECON record to EBCDIC 'FF'
- 6) STRING -- Add, Replace or Delete a string (up to 20 characters)
- 7) ORDER -- Place copies of specified RECON records from the set after the last legitimate RECON record but before the LAST-CARD.

UNCLASSIFIED

For the purpose of RECON record manipulations , 23 subfields were selected to provide the capability for altering different parts of the RECON records. These subfields were assigned 2-6 character acronyms for use on the Control Cards. These 'field specifications' give the ability to select particular fields. Of particular interest for this test are the D1, D2 and CW fields which affect dissemination and the CS field which affects the CHECKSUM itself. The complete list of allowable field acronyms follows.

DF	--	document format
DNSB1	--	" " " " number subfield 1
DNSB2	--	" " " " " " 2
DNSB3A	--	" " " " " " 3
DNSB3B	--	" " " " " " 3
ITEM	--	" " " "
PAGE	--	" " " "
DT	--	" " type
CL	--	classification
D1	--	dissemination 1
D2	--	dissemination 2
CW	--	code word
PD	--	publication date
EX	--	exemption category
TD	--	todate
PR	--	processing date
MG	--	management field
SN	--	series periodic set
SC	--	subject code in subject periodic set
CY	--	country code in " " " "
KW	--	keywords
TI	--	title
CS	--	checksum

The format of the Control cards is as follows.

COMMAND	COLUMNS	CONTENTS
USERID	1-6	USERID
	7	-
	8-22	new userid
AGENCY	1-6	AGENCY
	7	-
	8-11	new agency
REQNUM	1-6	REQNUM
	7	-
	8-11	new request number
BIT	1-6	BIT
	7	F or M or L (first, middle or last)
	8-13	field specification (acronym for which part of the RECON record to alter)
BYTE	1-6	BYTE
	7	F or M or L
	8-13	field specification
STRING	1-6	STRING
	7	F or M or L
	8-13	field specification
	14	A or D or R (add,delete or replace)
	15-34	string to add,replace with or delete (in case of delete the contents of the string are ignored -- the # of characters in the string will be the number of characters deleted from the RECON record)
		--OR--
		BLANK (set field to blanks)
		--OR--
		ZERO (set field to binary zeros)
ORDER	1-5	ORDER
	7	-
	8-80	continuous sequence of 2 digit numbers

UNCLASSIFIED

(max 36) representing an ordering of RECON records from the output set to be placed after the legitimate records but prior to the LAST-CARD.

(ex. 20051920 -- copy the 20th RECON record in the set and place it after the last RECON record in the set. Follow this with the 5th, 19th and 20th records (spelling the word TEST).)

Theoretically the program can handle any file size passed in. For practical purposes however, an input file size limit of 1000 records should be observed. The program will output the altered records to a data set picked up by the spanned record formatter Utility. It will also output a hardcopy count of processed control cards and any error messages that were generated due to improper Control cards.

UNCLASSIFIED

UNCLASSIFIED

Notes on Legitimate Traffic Modulation (LTM)

(1 February 1983)

ATTACHMENT D

UNCLASSIFIED

Notes on Legitimate Traffic Modulation



STAT

1 February 1983

Introduction

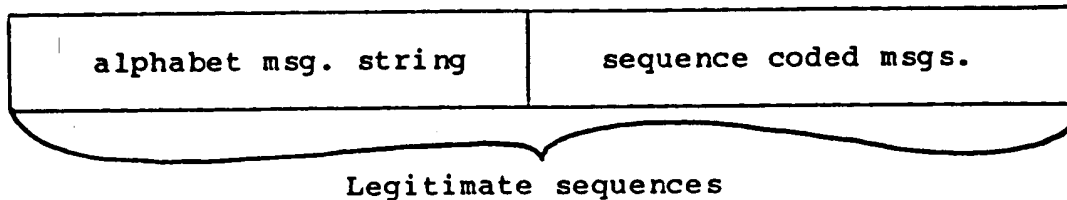
Legitimate Traffic Modulation (LTM) is one of the most formidable security problems encountered when data bases containing multilevel security and compartmented information are exposed (connected) to untrusted network access. At first glance, an LTM type clandestine attack would appear to offer an unlimited, uncontrollable bandwidth, since LTM involves the transmission of legal output but in a way as to encode information.

All covert signalling/timing channels can be fully exploited if tradeoffs on normal system/network operations and throughput are prohibited. The following discussion will suggest an approach to severely limiting the LTM available bandwidth, while defining the operational constraints on the target system.

This note contains a brief discussion of Legitimate Traffic Modulation and possible techniques for countermeasures. These techniques could be employed for any remotely accessed data bases where security is of prime concern. With some minor enhancement of the Guard system the LTM defenses of section I.B. 1, 4, below, could be employed for existing data bases. The sequence proof (encrypted data base) scenarios could not be applied to existing systems without extensive modification.

The sequence proof scenarios would require a verified, off-line, data base encryption peripheral. The Guard Device prototype design could serve this function, with minor modification. Properly accessed encrypted data bases may be a solution to LTM.

I. General Concepts: Legitimate Traffic Modulation (LTM)



A. Attack requirements:

1. sequence must be pre-ordered and known by receiver (attack method is sequence integrity dependent)
2. output sequence must have nonunique msg. types in trailer portion of response set, or
3. output sequence must have known spacings of unique msg. types in trailer portion
4. receiver must know relative transmit time (sensed by arrival time) of legitimate msgs. to exploit a timing channel attack

B. Defense:

1. limit length of response sequence (reduce channel bandwidth)
2. detector function
 - a. the principal detector function will be code detection
 - (1) various methods exist for this (decyphering techniques)
 - b. method (example)
 - (1) entire response msg. set must be buffered prior to output
 - (2) alphabet string detection
 - (a) each 1 to n string of msgs. will be examined with the resultant trailer sequence

(3) patterns to be detected

- (a) alphabet strings: with unique msg. types
- (b) trailer strings: all previously encountered msg. types

(4) actions taken

- (a) buffer deleted when (above) clandestine code probabilities are encountered

3. Buffered response set will be scrambled

- a. order of response msgs. will be changed randomly
- b. order of response msgs. will be changed by predetermined algorithms
- c. this appears to be most effective LTM countermeasure
 - (1) ease of implementation
 - (2) effectiveness
 - (3) can be standard output sequence function not requiring code ident (as in Section I.B.2 above)

4. Guard controlled (relative transmit timer for incoming queries and outgoing responses will nullify the use of timing modulation (the activator of the timing attack cannot control the relative time of msg. transmission)

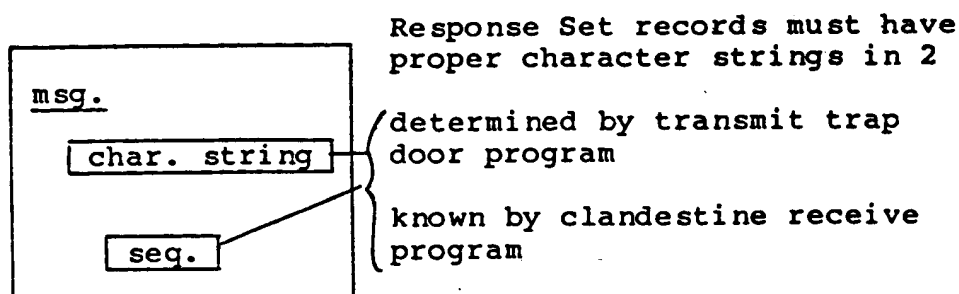
- a. this feature could be implemented by polling or time-slot transmission. (Guard would control random utilization of transmit time slots.)

II. Problem: (Sequence Proof) LTM Channel

A. Trap door program function

From the set of responses

1. scan response set for records with
 - a. appropriate characters in predetermined string field
 - b. appropriate characters in predetermined sequence character field
2. transmit related records (this activates LTM channel)



3. receive program decodes clandestine message from the received response set

B. Constraints on defensive measures

1. Must not disrupt communication link throughput rate
2. Must not decrease response set received

III. Solution: (Sequence Proof) LTM Channel

A. Requirements for attack:

1. trap door program must know contents of records which will be transmitted
2. location of data and sequence information fields and/or pointers must be known to transmitter and receiver
3. trap door program must select, from response set, those records having proper characters in the predetermined data and sequence fields

B. General solution:

1. encrypted data base with header and trailer information stripped on output (trap door cannot know information released)
2. limit response set size

C. Solution (using Guard concept) when query capability is required:

- 1.(a) queries could search on header information only (header would contain key words for query search). Thus severely restricting the amount of characters usable by a trap door program
- (b) or incoming query (search parameters) encrypted with appropriate key (or single key if 1 key scenario is used)
- (c) thus query can only search/hit on appropriate records (if multi-key scenario is used)

2. Scenario:

- Enter:
1. auth and save store encryption results and auth (at update device)
 2. now no way to tell what output will be from internal trap door. Thus trap door cannot select sequence or character string of response set for output because it cannot know what will be output

- Exit:
1. decrypt at (on-line device)
 2. authenticate as before
 3. scramble response set
 4. Guard determines destination and strips headers and trailers (only encrypted text is passed after decryption by Guard)
 5. Guard checks contents of response set (i.e., response set must contain more than 1 record, and response set must contain no identical records)

IV. Conclusions

As discussed in part III.C.2, above, an encrypted data base can prevent a trap door program from knowing which data is transmitted. This is because encryption/decryption of text is done off line (outside of operating space of the data base or the target system). No plain text data arriving at the Guard is transmitted (headers are stripped). No encryption data is transmitted (encrypted text changed to plain text at Guard before transmission). Thus the Guard functions as an output sequence scrambler and also functions as an encryption device. Although not applicable to the present RECON system (the RECON data base is not encrypted), new data bases employing this scenario with a Guard Device concept may be protectable in this manner.

LTM attacks are sophisticated and require a high level of target system penetration. It was the decision of the RECON/Guard Program Manager that the Guard Device concept could be fully evaluated without incorporating LTM defensive capabilities other than response count limit manipulation (Section I.B.1) for the RECON application of the Guard Device system.

This communication suggests approaches to controlling a covert signalling channel attack utilizing LTM. The proper use of the Guard Device System (i.e., output sequence scrambling plus encryption, and/or response record sequence sampling, can cause the bandwidth of a LTM type attack to be severely limited or eliminated.

UNCLASSIFIED

COINS/HAS Implementation Schedule
(11 August 1983)

ATTACHMENT E

UNCLASSIFIED

12. Test of 64kb lines on C30 | CI | Approx a couple of days to iron out any problems if things go smooth. (monitor at NCC)
 | MI |
 | IO |
 | I |
13. C30/PDP1170 connection test (C30) | CI | Approx amount of test time required 4 hrs.
 | PI |
 | MI |
 | IO |
 | I |
14. RPO6's delivery to CIA | CI | Approx delivery date 09/___/83
 | PI |
 | MI |
 | IO |
 | I |
15. Disk Format and test RPO6 | MI | Approx amount of time needed 3 days.
 | CI |
 | CI |
 | I |
16. Unix Installation | LI |
 | IO | Start 10/___/83 and be completed 10/___/83
 | CI |
 | I |
17. Shipment of a MOD40 to CIA | CI | Ship Terminal from CPMO, Used during Software Installation and Acceptance test. Temporary LOAM until Installation is complete.
 | MI |
 | IO | Ship Date 08/___/83, arrival 09/___/83
 | I |
18. Installation of Mod40 by 1170 console | CI | Approx time required few hrs.
 | PI |
 | MI |
 | IO |
 | I |
19. Connect/Test Mod40 at 1170 console | CI | Approx time required few hrs.
 | PI |
 | MI |
 | IO |
 | I |
20. HAS 5.0 Installation | LI | Approx time required 3 days
 | IO | Start date ___/___/83 and complete ___/___/83
 | CI |
 | I |
21. Mini Test of HAS 5.0 Software | CI | Test will be conducted to assure the HAS can communicate with other Host on the COINS Network.
 | PI |
 | MI | Approx time required 2 days.
 | IO |
 | I |
22. Installation of NAS-software interface to RECON | LI | Start ___/___/83 and Complete ___/___/83
 | IO |
 | CI |
 | I |
23. Test of NAS Software Interface to Recon | LI | Joint testing with LOGICON/SYTEK Starting ___/___/83
 | IO | Completing ___/___/83
 | CI |
 | I |

24. Addr/Host | CI
 Changes For | PI
 Rytip (N) | MI Submitted Request ___/___/83 Completed ___/___/83
 INI (N) | IOI " " ___/___/83 " ___/___/83
 Switch (D) | I " " ___/___/83 " ___/___/83
 DIA (D) | I " " ___/___/83 " ___/___/83
 PAC (D) | I " " ___/___/83 " ___/___/83
 ADCOM (D) | I " " ___/___/83 " ___/___/83
 TAS COINS(L) | I " " ___/___/83 " ___/___/83
 NSH " (L) | I " " ___/___/83 " ___/___/83
 TRF " (L) | I " " ___/___/83 " ___/___/83
 TAS NISC (L) | I " " ___/___/83 " ___/___/83
 TAS STATE(L) | I " " ___/___/83 " ___/___/83
 TAS DIA (L) | I " " ___/___/83 " ___/___/83
 TAS LLL (L) | I " " ___/___/83 " ___/___/83
 HAS NPIC (L) | I " " ___/___/83 " ___/___/83
 HAS CIA (L) | I " " ___/___/83 " ___/___/83

25. Request BLK | CI Based on the number of ports found on the DH.
 of Solis | PI Requested ___/___/83
 ID's | MI Request Granted ___/___/83 and Numbers received ___/___/83
 | IOI

26. Request | CI Request of F1432
 Solis Soft/ | PI Submitted request on ___/___/83
 TIDS updated | MI Request Granted ___/___/83 completed ___/___/83
 | IOI

27. Update of | LI Request LOGICOM to update the Logical Terminal (LTR)
 LTR File | IOI numbers in TAS Software.
 | GI

28. Trigraph CIC | MI Request Submitted ___/___/83
 to be added | SI Request Completed ___/___/83
 SOLIS ,FE | AI

29. Test FE/INI | CI Approx amount of time required 3 days.
 Software | PI (morning hours)
 changes | MI
 | IOI

30. Operator Imp | MI Approx amount of time required 2-3 (4hr.) days.
 Training | CI
 | CI

31. Operator TAS | LI Approx amount of time required 2 weeks.
 Training | IOI
 | GI

32. Appoint an | CI Appointed ___/___/83
 ISSU | II
 | AI

33. AAF4/ISSU | PI Approx amount of time required 2 days.
 Training | MI
 | IOI
 | I

34. Operational ICI Approx amount of time required 3-4 days.
Acceptance IPI
test by IMI
COINS IOI
I I
35. Mod40/Loan ICI Approx. date of return 11/___/83
returned IPI
IMI
IOI

UNCLASSIFIED

Memorandum of Understanding

CIA/COINS-PMO

(3 June 1983)

ATTACHMENT F

UNCLASSIFIED

3 June 1983

MEMORANDUM OF UNDERSTANDING

1. OBJECTIVE

This memorandum delineates the division of responsibility between the COINS PMO and CIA for the RECON/GUARD project. The COINS PMO is providing the necessary hardware and software for the Host Access System (HAS) for the testing and evaluation of the project. The CIA is providing the space and relevant personnel and software for the GUARD testing. The project is to be tested in phases. In the event that any of the phases prove unsatisfactory based on the evaluation presented to CIA management, the project will be terminated and the equipment returned to the COINS PMO.

It is important to state that this agreement supports only the testing of the RECON/GUARD system. The provisions of the MOU will terminate following the completion of this test or at the discretion of either party. In addition, this agreement does not imply any other commitment by either party. There will be no connection of CIA central computer services to any external networks without written approval by the Office of Data Processing, the Office of Security, and the data base owner as appropriate.

3. DIVISION OF RESPONSIBILITY

a. Responsibilities of the COINS PMO

(1) Fund procurement and installation of the PDP 11/70 system for use as the HAS, including peripheral equipment and terminal interface device. The HAS will be configured for 16 user terminals, with future expandability to 32.

(2) Assemble and monitor PDP 11/70 acceptance test procedures to be run by CIA personnel.

(3) Procure and install UNIX/PWB operating system.

(4) Install HAS software, customized for connection to CIA GUARD computer, and including handler program for CIA Delta Data Terminals (or use HAS supplied terminals).

(5) Procure, install and test the C30/IMP at CIA, connect the IMP to the COINS II network, and conduct performance acceptance testing. The COINS PMO will provide for hardware and software maintenance of the IMP.

(6) Connect HAS to C30/IMP and to GUARD System.

(7) Supply fully cleared software contractor on call who will be responsible for continuing maintenance of the HAS software. When centralized network down-line diagnostic and maintenance capabilities become available, this contractor may no longer be required. The contractor may be located on-site for the first 45-90 days.

(8) Provide and supervise integration acceptance testing to insure that HAS is fully functional and that all system interfaces are operating as intended.

(9) Train CIA computer operators to run and manage the HAS.

(10) Write two programs to format the data retrieved from RECON for use by users, including provisions to insert security classification and handling instructions at the top and bottom of each page.

b. Responsibilities of the CIA

(1) Provide space and proper environmental conditions for installation of the HAS and C30/IMP. This space must be in a TOP SECRET SI/TK protected area.

(2) Run two 64KB lines from the TETRAHEDRON node at the CIA communications center to the CIA C30/IMP location.

(3) Receive the PDP 11/70 system from DEC and supervise its installation.

(4) Provide proper power, air conditioning, conduit and other installation-related support as necessary.

(5) Perform acceptance tests on the PDP 11/70 in accordance with procedures provided by the COINS PMO.

(6) Supply full-time operators for the HAS. These operators will be trained in HAS and IMP operations by the COINS PMO.

(7) Contract for maintenance of the PDP 11/70 hardware and provide for stocking of hardware-related supplies, e.g., disk packs, magnetic tapes, paper, etc...

(8) Provide suitable work space for the cleared software maintenance contractor supplied by the COINS PMO to work on-site for initial 45-90 days of operations.

(9) Select an individual to serve as Information System Security Officer (ISSO) for the HAS. This person will be responsible for security of the HAS, maintenance of CIA user access authorization tables in the HAS, and assurance that HAS terminals are operated in accordance with CIA and COINS security regulations.

(10) Execute, in cooperation with the COINS PMO, the prepared acceptance test plan for the HAS once it is ready for operational use.

(11) The RECON system will be responsible for sorting the records retrieved for each answer before the records are transferred to the HAS for formatting and output.

4. Dependent upon the results of the testing of the RECON/GUARD, additional responsibilities will be negotiated between the CIA and COINS PMO.

~~Concurrences:~~

STAT